



Effective Date: 6/1/17

Remote Access Standard

Purpose

The Remote Access Standard is applicable for access to all DET/State information systems, system environments, and/or DET/State information.

This standard is intended to facilitate the attainment of the Access Control Policy and associated Information Technology (IT) Security Policy objectives.

Standard

Remote access to DET/State information systems, system environments, and/or information is allowed provided there is a documented business need (i.e. remote access required for job duties) and appropriate access, authorization, and security measures are in place.

- Remote access requests must be approved by an individual's DET Section Supervisor, the Section Chief, or a DET Bureau Director (AC-2).
- Remote access must be limited to only those systems necessary for identified and approved functions (AC-3).
- Remote access to systems that contain classified information, as defined by the Data Classification Standard, must utilize multifactor authentication prior to allowing access to the information and the data must be encrypted in transit (AC-17).
- Non-State-owned equipment, including personal equipment (bring your own device - BYOD), used to connect to DET/State information systems, system environments, and/or information must meet the requirements of enterprise-owned equipment for remote access (AC-20).
- Non-State-owned equipment, including personal equipment (bring your own device - BYOD), cannot be used to access regulated data, i.e. personally identifiable information (PII) or Federal Tax Information (FTI)(AC-20).
- When actively connected to the DET/State network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped. Split-tunneling is not permitted (SC-7).
- Remote access is removed upon termination of employment or when an individual no longer requires the functionality for business needs (AC-2, AC-3).
- Remote access service offerings (virtual private network, virtual desktop infrastructure, etc.) will be set up and managed by DET Bureau of Infrastructure Support personnel.
- Network access control points that allow remote access must be monitored for security-related vulnerabilities and identified vulnerabilities must be remediated in accordance with the appropriate policy (e.g. Maintenance, Configuration, Incident Response) (AC-17).

Effective Date: 6/1/17

- Sessions must be automatically terminated as documented in DET procedures (AC-12, AC-17, SC-10).
- Remote sessions must be locked after upon user input or a maximum inactivity period of 15 minutes. (AC-2, AC-12).
- Authorized administrators must be able to lock, disconnect, or disable remote access sessions (AC-17).
- Regulated data, i.e. personally identifiable information (PII) or Federal Tax Information (FTI) cannot be stored or accessed from outside the United States (AC-17).
- Remote access for third-parties and vendors must comply with all DOA/DET policies and standards.
- Remote access should be defined in vendor/third-party contracts.
- Any remote access solution that does not meet this standard must seek and have an exception approved via the DET Exception Procedure for to access DET/State information systems, system environments, and/or information (AC-17).

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- BYOD - Bring your own (personally-owned) device.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.
- Multi-factor Authentication - Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
- Remote access - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet) (NIST 800-53 Rev. 4, Appendix B).

Compliance References

IRS Pub. 1075

NIST 800-53 Revision 4

Effective Date: 6/1/17

Exception Process

Exceptions to this and all DET Security policies, standards, and procedures must follow the DET Exception Policy and Procedures.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	7/1/2016	Original	Tanya Choice Cybersecurity Compliance Consultant
1.0	5/25/17	Final Approval	Bill Nash CISO

Authorized and Approved by:

Bill Nash



5/24/17

Print/Type

Signature

Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer